THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of authenticating a pair of correspondents in a communication system, said method comprising the steps of:
Exchanging cryptographic keys between said corespondents, said exchange being based on a public key mutual authentication scheme; and
using said keys for encrypting data in a symmetric-key data exchange.

2. A method as defined in claim 1, a first of said correspondents being a mobile station and a second of said correspondents being a base station.

3. A method as defined in claim 2, said mutual authentication including the steps of:
said base station transmitting a short term public key along with an identifier to said mobile station;
said mobile station combining its private key with said base station session public key and generating a pair of shared secret keys therefrom wherein a first of said keys is used for mutual authentication between said mobile station and said base station and a second of said keys is used for establishing a secret session key.

4. A method as defined in claim 3, including the steps of:
said mobile station computing an authentication string using the first of said keys and transmitting same to said base station as a registration request.

5. A method as defined in claim 3, including the steps of :
said base station retrieving said mobile station public key and using said mobile station public key and its short-lived private key for computing a second pair of shared secret keys;
comparing said first keys; and
computing a pair of session keys for transmission to the mobile station.

6. A method for mutual authentication between a base station and a mobile station comprising the steps of:

the mobile station authenticating itself to the base station using its private key;

the base station authenticating itself to the mobile station using the mobile station's public key obtained by said base station from a trusted correspondent.